DAVID L. ANDERSON (CABN 149604)
United States Attorney

HALLIE HOFFMAN (CABN 210020)
Chief, Criminal Division

MICHELLE J. KANE (CABN 210579)
KATHERINE L. WAWRZYNIAK (CABN 252751)
Assistant United States Attorney

1301 Clay Street, Suite 340S
Oakland, California 94612
Telephone: (510) 637-3680
FAX: (510) 637-3724
michelle.kane3@usdoj.gov
katherine.wawrzyniak@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. YEVGENIY ALEXANDROVICH NIKULIN, Defendant.	No. CR 16-00440 WHA **UNITED STATES' SENTENCING MEMORANDUM** Hearing Date: September 29, 2020 Time: 2:00 p.m. Courtroom 12, 19th Floor

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTRODUCTION

Defendant Yevgeniy Nikulin is to be sentenced for his convictions on nine counts arising from his sustained hacking campaign affecting computer users around the world. From behind a keyboard in Moscow, Russia, Nikulin gained access to the computers of at least four U.S. companies, including victims based in the Northern District of California. To do so, he used the identities of individual employees while installing malicious software on the victims' computers. Nikulin stole millions of user credentials, which he sold for profit and shared with fellow hackers. His conduct left those users vulnerable to other crimes, including fraud and identity theft. Nikulin himself used some of the information he stole to perpetrate further crimes.

As the victims testified at trial, computer intrusions like Nikulin's impose devastating costs on businesses and individuals. Someone like Nikulin can work in anonymity, half a world away, profiting off his attacks on U.S. companies while insulating himself from consequences. Identifying a cybercriminal like defendant and bringing him to justice – which is the rare success story – requires a massive effort by U.S. law enforcement. It is therefore imperative to deter other would-be cybercriminals around the world by sending a clear message that attacking and victimizing the United States' economy will result in severe penalties.

Moreover, defendant himself poses a significant risk of committing further crimes. Defendant has expressed no remorse or regret for his actions. He will return to Russia when he is released from custody and will once again be outside the reach of U.S. law enforcement. The Court should impose a sentence that will prevent Nikulin from resuming his crimes for a long time.

For all these reasons, the United States respectfully recommends that the Court sentence defendant Nikulin to a term of 145 months of imprisonment, which, as specified in the PSR, includes terms of 61 months on each of Counts Two, Six, and Eight and 60 months on each of Counts One, Four, Five, and Seven, to run consecutively to each other, and 24 months on each of Counts Three and Nine, to run concurrently to each other and consecutively to all other counts. This sentence represents the low end of the applicable Guidelines range. The Court should also sentence defendant to a three year term of supervised release on Counts One, Two, and Four through Eight, and a one year term of supervised release on Counts Three and Nine, to run concurrently. Finally the Court should award restitution to the

victim companies as recommended in the PSR.

BACKGROUND

The Court is familiar with the facts of this matter, having presided over the recent trial. Accordingly, the following discussion highlights the facts and issues most relevant to the sentencing considerations of 18 U.S.C. § 3553(a).

A. Offense Conduct

The evidence introduced at trial proved that, beginning in early 2012, defendant targeted LinkedIn Site Reliability Engineer Nick Berry. He put a malicious shell called "madnez" on Mr. Berry's personal computer, which allowed him to send commands to the computer remotely. Because Mr. Berry used that computer to access LinkedIn's corporate network via Virtual Private Network ("VPN"), defendant was able to obtain Mr. Berry's login credentials. He eventually was able to log on to a LinkedIn production server using Mr. Berry's credentials and exfiltrate data for millions of LinkedIn users, including email addresses, "hashed" passwords, and other data.

LinkedIn discovered the intrusion when someone posted a portion of the hashed passwords on an online hacking forum, seeking help cracking them. Both Bruno Connelly and Ganesh Krishnan testified about LinkedIn's response, including the steps taken to determine how the then-unknown attacker had gained access to their network, and how to remediate the damage. Evidence from the computer of accused hacker Oleksandr Ieremenko showed defendant sharing stolen LinkedIn data with Ieremenko later the same year.

The evidence also showed that defendant obtained login credentials to Dropbox's corporate system for employee Tom Wiegand, because Mr. Wiegand had used the same password on LinkedIn and Dropbox. Once he was able to access Dropbox's system as Mr. Wiegand, he gave himself access to Dropbox document repositories, including a set of Dropbox user credentials with email addresses and hashed passwords. The FBI alerted Dropbox to the possible threat based on evidence from its LinkedIn investigation. Cory Louie of Dropbox testified about the significant response mounted by Dropbox to investigate and remediate the attack.

Evidence introduced at trial further showed that defendant attacked Formspring's corporate network using credentials for employee John Sanders that he found through a compromise of Mr.

Sanders' Dropbox account. Using Mr. Sanders' Formspring credentials, defendant again installed the malicious software on Formspring's system and exfiltrated a set of user credentials. Formspring discovered the breach when credentials were posted to the same Internet forum. Founder Ade Olonoh testified to the effect the attack had on his company and the work its employees undertook to repair the damage. Evidence from email accounts and Western Union showed that defendant worked with co-conspirators to sell the stolen Formspring user credentials later in 2012.

The government also introduced evidence that, in 2013, defendant attacked Automattic's computer systems, compromising the identities of several employees. Evidence from defendant's Google account showed him systematically searching for information about those employees online, targeting them as he had targeted the victims at LinkedIn, Dropbox, and Formspring.

Defendant's method of operation throughout the four attacks was consistent – targeting engineering employees with high-level access through Internet research, compromising employee credentials, installing malicious software to maintain access, researching corporate infrastructure through access to internal documentation, and exfiltration of valuable user credentials. All through this campaign of intrusions, database thefts, and trafficking the results, defendant used various online identities in an effort to hide his involvement. The FBI's painstaking investigation unmasked the defendant by systematically connecting each fake account through victim logs, subscriber records, account contents, and other documentary evidence.

B. Procedural History

Defendant was indicted on October 20, 2016, following his arrest in the Czech Republic at the request of the United States, supported by a provisional arrest warrant. Defendant is a citizen and resident of Russia, but according to news reports, was in the Czech Republic on a vacation. He was held in custody while the United States' request for his extradition was litigated. He was eventually ordered extradited and made his initial appearance in the Northern District of California on March 30, 2018.

Trial commenced March 9, 2020, with jury selection. Two days of opening statements and testimony followed. After a break in proceedings due to the public health emergency, trial resumed on July 6, 2020. The government rested its case on July 9, 2020, and defendant declined to present evidence. Closing arguments were held on July 10, 2020.

After approximately six hours of deliberations, the jury returned guilty verdicts on all nine charged counts: three counts of computer intrusion, in violation of 18 U.S.C. § 1030(a)(2)(C) (as to LinkedIn, Dropbox, and Formspring), two counts of causing damage to a protected computer, in violation of 18 U.S.C. § 1030(a)(5)(A) (as to LinkedIn and Formspring), two counts of aggravated identity theft, in violation of 18 U.S.C. § 1028A (as to employees of LinkedIn and Formspring), one count of conspiracy, in violation of 18 U.S.C. § 371 (as to trafficking of Formspring's credentials), and one count of trafficking in stolen access devices, in violation of 18 U.S.C. § 1029(a)(2) (as to Formspring's credentials). The jury also agreed that the government had proven at least one aggravating factor increasing the maximum penalties for the violations of 18 U.S.C. § 1030(a)(2) from one year of imprisonment to five years for Counts One, Four, and Seven, and increasing the maximum penalties for causing damage to a protected computer from one year of imprisonment to ten years for Counts Two and Eight.

SENTENCING GUIDELINES

A. Guidelines Calculation

The United States agrees with the Sentencing Guidelines calculation in the PSR:

Counts One, Two, Four through Eight:

a.	Base offense level: U.S.S.G. § 2B1.1(a)(2), 2X1.1	6
b.	Specific offense characteristics:	
	U.S.S.G. § 2B1.1(b)(1)(I) – Amount of Loss: more than $1,500,000	+16
	U.S.S.G. § 2B1.1(b)(10) – Sophisticated Means	+2
	U.S.S.G. § 2B1.1(b)(11)(B)(i) – Trafficking of unauthorized access devices	+2
	U.S.S.G. § 2B1.1(b)(18) – conviction under 18 U.S.C. § 1030(a)(2)(C) and intent to obtain personal information	+2
	U.S.S.G. § 2B1.1(b)(19)(A)(ii) – Conviction under 18 U.S.C. § 1030(a)(5)(A)	+4
c.	Adjusted offense level	32
d.	U.S.S.G. § 3D1.2(d) – Adjusted offense level after grouping	32
e.	Total offense level	32

Counts Three and Nine:

a. U.S.S.G. § 2B1.6(a) – Aggravated Identity Theft	24 months consecutive to any other sentence

With a criminal history category of I, the result is a Guidelines range of 121 to 151 months of imprisonment on Counts One, Two, Four through Eight and 24 months consecutive on Counts Three and Nine.

B. Defendant's Objection to the Guidelines Calculation

Defendant objected to the loss figures in the draft PSR. Defendant has not provided an alternative loss calculation. Based on the available evidence, the Court should accept the estimate of loss in the PSR. First, the Court need only make a reasonable estimate of the loss, as noted in the commentary to Guidelines. Moreover, as incorporated in the revised final PSR, the victims have provided more thorough explanations of their losses through Victim Impact Statements. In addition, the witnesses who testified at trial on behalf of the victims provided sufficient basis for the Court to find that the reported loss amounts are reasonable estimates.

1. Reasonable Estimate of Loss for Offenses Under 18 U.S.C. § 1030

The parties and the PSR are in agreement that U.S.S.G. § 2B1.1 governs sentencing in this case. Under section 2B1.1, the base offense level increases based on the amount of loss. U.S.S.G. § 2B1.1(b). The Commentary to section 2B1.1 defines loss as the "greater of actual loss or intended loss." U.S.S.G. § 2B1.1, cmt. n. 3(A). In this case, the PSR uses "actual loss," which typically means the "reasonably foreseeable pecuniary harm that resulted from the offense." *Id.* at cmt. n. 3(A)(I). For cases involving a violation of 18 U.S.C. § 1030, however, the Commentary contains a special provision regarding loss, which states:

> Offenses Under 18 U.S.C. § 1030.—In the case of an offense under 18 U.S.C. § 1030, actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: any cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.

U.S.S.G. § 2B1.1, cmt. n. 3(A)(v)(III). Thus, the Court may consider the types of pecuniary harm

described by the victims in their statements and testimony, forseeable or not, in calculating the loss amount under section 2B1.1 in this case.

That calculation need only be a "reasonable estimate of loss, given the available information." *United States v. Tadios*, 822 F.3d 501, 503 (9th Cir. 2016) (citation omitted) (upholding loss amount based on estimate of employee's wrongly-claimed salary); *see also* U.S.S.G. § 2B1.1, n. 3(C) ("The Court need only make a reasonable estimate of the loss. The sentencing judge is in a unique position to assess the evidence and estimate the loss."); *United States v. Borrasi*, 639 F.3d 774, 784 (7th Cir. 2011) (acknowledging that government has burden to prove loss but that defendant must come forward with substantiated evidence, not "vague valuations" to refute the government's proof; *United States v. Rigas*, 583 F.3d 108, 120 (2d Cir. 2009) (upholding district court's estimate even though it could not determine the "precise amount" of the loss attributable to defendants' fraud,); *United States v. Uddin*, 551 F.3d 176, 180 (2d Cir. 2009) (finding loss calculation reasonable in food stamp fraud case where district court used multiple estimates including average dollar amount of food stamp redemptions at similar stores, witnesses' observations of defendant's store, and estimate of percentage of transactions that were actually fraudulent).

2. Evidence Regarding Losses Suffered by the Victims

Sunnyvale-based LinkedIn Corporation has submitted a Victim Impact Statement establishing that it spent at least $2 million responding to defendant's attack and exfiltration of data. The total cost reflects its internal incident response and consultation with external vendors. According to the statement:

> LinkedIn addressed the breach by (1) notifying the owner of any potentially compromised account, (2) investigating the breach itself, and (3) remediating the company's systems and procedures to prevent further unauthorized access by the hacker. This effort required a company-wide response, including employees from Operations, Engineering, Product, Marketing, Legal, Human Resources, Security, and Customer Support. Due to the 24/7 nature of the response effort and the magnitude of Mr. Nikulin's breach, many employees had to work significantly increased hours for the two-month period. Furthermore, LinkedIn hired external security and IT vendors to investigate the breach, conduct security assessments, and reveal any potential vulnerabilities in LinkedIn's system.

This statement is supported by the sworn trial testimony of both Bruno Connelly and Ganesh Krishnan. Importantly, LinkedIn notes that its estimate is extremely conservative, and based solely upon the expenditures they could document. After eight years, this resulted in a claimed loss amount that was

less than the actual amount spent responding to the offense.

Mr. Connelly testified that when LinkedIn discovered the breach, it established a "war room" in which 40 to 50 people worked to help with the response. Trial Transcript ("Trial Tr.") at 31:12-16. He testified that the people working on the response had roles "across all parts of engineering" as well as the security team. Trial Tr. at 31:19-22. Mr. Connelly explained that the incident was the highest level of critical – "code red" – which meant that it was an "existential risk" for the company. Trial Tr. at 32: 20-23. He testified at length about the multi-step process that the company went through to track the attacker through the LinkedIn system, including by review of VPN logs to identify anomalous activity. E.g., Trial Tr. at 43:24-44:9. Mr. Connelly explained that the identification of particular IP addresses led to multiple investigations by the Code Red team to look at the usage on the LinkedIn public platform. Trial Tr. at 44:21-25. Mr. Connelly explained how the internal team used the IP addresses to identify suspicious browser cookies and unusual user agent strings, which all together formed a "fingerprint" of the attacker. E.g., Trial Tr. at 50:3-51:6. He testified that LinkedIn identified over 30 LinkedIn customer accounts that had unauthorized access by the attacker using this "fingerprint." Trial Tr. at 51: 23-52:10. In addition to the customer accounts, the Code Red team followed the attacker's path through the LinkedIn corporate network, including access to the Oracle database machines where user credentials were stored. Trial Tr. at 57: 12-24.

Mr. Connelly testified that LinkedIn spent approximately six weeks remediating the attack, including dealing with compromised member accounts. Trial Tr. at 73:16-75:24. He testified that LinkedIn spent "significantly" more than $5,000 (the jurisdictional threshold) responding to defendant's attack, that approximately 100 employees were ultimately involved, that those employees were diverted from doing other business activities, and that is was the most serious data breach that he has worked on. Trial Tr. at 75:25-76:24.

Ganesh Krishnan of LinkedIn also testified to the company's incident response. He described the steps, which included verifying that the password hashes actually belonged to LinkedIn, figuring out the extent of the breach, determining whether the breach was still occurring, and identifying remedial steps. Trial Tr. at 289:1-9. Mr. Krishnan noted that it was "all hands on deck" with employees across the company working on the "Code Red." Trial Tr. at 288:2-11. He also confirmed that LinkedIn hired an

outside consultant to assist with the incident response. Trial Tr. at 296:19-22. He explained that LinkedIn viewed the stolen data as valuable and said that it was the most important issue at LinkedIn at the time. Trial Tr. at 288:2-25. Like Mr. Connelly, Mr. Krishnan testified that this was the most significant data breach that he worked on. Trial Tr. at 297:6-8. He confirmed Mr. Connelly's account that the investigation lasted a few months and the remedial steps lasted "longer after that." Trial Tr. at 296:15-18.

San Francisco-based Dropbox, Inc., has submitted a Victim Impact Statement describing how the company:

> …expended significant internal resources to investigate the scope of Mr. Nikulin's intrusion into its systems and the damage caused. The team of employees who dedicated their time and energy to this investigation and mitigation effort did so at the expense of otherwise working on improving and developing Dropbox's products. Dropbox also incurred infrastructure costs to remediate systems affected by Mr. Nikulin's criminal conduct. Additionally, Dropbox hired external forensic vendors and attorneys to assist in the investigation.

Dropbox has conservatively estimated that its costs in responding to defendant's attack was at least $514,000. The testimony of Cory Louie, former head of Trust and Security for Dropbox supports this estimate. Mr. Louie testified that, when he began working at Dropbox, the company had begun responding to its discovery of the breach. Trial Tr. at 79:19-22. He explained that Dropbox also had a "war room." to investigate the attack. Trial Tr. at 85:10-17. Mr. Louie testified that it was "all hands on deck," with employees working to determine what had happened while securing the company infrastructure from further attacks. *Id.* He estimate that 20 to 25 employees actively worked on the response, and that those people were leaving aside their other jobs to do so. Trial Tr. at 86:4-14. Mr. Louie was brought in to lead and coordinate the response, investigation, and recovery. Trial Tr. at 86:15-18. Dropbox determined that multiple corporate accounts had been compromised using IP addresses originating in Russia. Trial Tr. at 86:18-87:12. Mr. Louie testified about how Dropbox identified the corporate accounts using the suspicious IP addresses and a unique identifier called GVC that could trace activity by one computer across multiple Dropbox logins. Trial Tr. at 89:5-90-17. He testified about the process Dropbox employees used to follow the attack through its systems via activity logs for the compromised accounts and how those activity logs showed access to the account belonging to Tom

Wiegand, which contained a file with a subset of usernames and hashed passwords. Trial Tr. at 94:10-25.

San Francisco-based Formspring, which is now defunct, has submitted a Victim Impact Statement outlining $20,000 in losses as the result of defendant's conduct. The statement describes approximately $15,000 in engineering resources and approximately $5,000 in messaging and new infrastructure. The statement also notes that "[t]his incident had an impact on our brand, and the trust our users had in us to protect their data. We had thousands of users delete their Formspring accounts shortly after the incident." The losses are supported by the testimony of founder Ade Olonoh.

Mr. Olonoh testified that Formspring first learned of the breach upon being contacted in July 2012 by someone who had seen the posting of approximately 420,000 Formspring credentials to an Internet forum. Trial Tr. at 106:5-18. At the time, Formspring had about 30 million registered users and approximately 20 employees. Trial Tr. at 89:22-90:13. Mr. Olonoh testified about the process that Formspring went through to investigate the potential breach. He explained how he verified that the posted credentials actually belonged to Formspring users. Trial Tr. at 108:13-109:21. Mr. Olonoh then described how Formspring combed through a "large volume of system logs" to understand what "vector" had been used in the attack. Trial Tr. at 109:22-111:12. He testified about the "chaotic" environment in the Formspring office as "everybody from the engineering team" was investigating the attack and a support team was "busy responding to user questions and concern about the hack." Trial Tr. at 127:20-128:3. He testified that after they had figured out what happened the next step was to secure the compromised server, send messages out to all Formspring users, write new code, and rebuild the development server. Trial Tr. at 128:4-21. Mr. Olonoh estimate several hundred to over a thousand employee hours were spent on the response, and certainly over the $5,000 jurisdictional threshold. Trial Tr. at 128:22-129:10. Formspring was much smaller at the time than LinkedIn or Dropbox, so even an "all hands on deck" (Trial Tr. at 128:3) situation resulted in significantly smaller losses than those of the other victims, although the attack had a major impact on the company. Mr. Olonoh testified to the fact that many users deleted accounts following the publicity of the breach. Trial Tr. at 131:1-10. Formspring employee John Sanders whose credentials defendant used to infiltrate the corporate system, testified to the "panic" and "anxiety" he felt as a young employee, new to the industry, whose account had been

compromised and put the company at risk. Trial Tr. at 72: 8-19.

Automattic has estimated its loss amount as $250,000. Automattic is the parent company of Wordpress.com and other online services. FBI Special Agent Jeffrey Miller testified at trial regarding the scope of the intrusion into Automattic's system, which included multiple compromised employee accounts. Trial Tr. at 525:7-532:5; 557:18-558:23. He described the extensive logs gathered by the company, a summary of which was admitted at Exhibit 17A. Given the estimates by the other victims, Automattic's estimate is within the expected range of reasonable expenditures. Automattic has represented that the company is attempting to gather information regarding its losses. The United States will provide that information if it is received before sentencing.

Altogether, the evidence provided by the victims for sentencing and the evidence introduced at trial supports the loss figure in the PSR as a reasonable estimate, and likely understatement, of the costs to the victims.

UNITED STATES' SENTENCING RECOMMENDATION

The United States' recommended sentence of 145 months of imprisonment is substantively reasonable and sufficient, but not greater than necessary, to address the factors set forth in 18 U.S.C. § 3553(a).

A. Nature and Circumstances of the Offense

Defendant's attacks created existential crises for the victim companies. As discussed above, each company expended massive resources responding to his intrusions, pulling employees and resources from their ordinary functions. Moreover, we know that defendant himself used the stolen LinkedIn data to compromise at least 30 customer accounts identified by LinkedIn in its own investigation. He may have targeted those individuals based on their professional positions with the goal of hacking their companies and selling that data.

Far more than that, however, his conduct left millions of users vulnerable to further crimes by the people with whom defendant shared their personal information. Special Agent Miller testified about the uses for stolen data, including accessing bank accounts, hacking email accounts, and spam advertising. Trial Tr. at 625: 19-24. He testified that even when companies protect passwords through hashing, there are individuals who specialize in cracking those passwords for profit. Trial Tr. at 625:25-626:6. Special

Agent Miller explained that user credentials are most valuable when first stolen, that the value diminishes as the breach becomes public, and that data is sold multiple times at declining prices through dark markets. Trial Tr. at 626:13-627:4. The LinkedIn data would have been the most valuable of all the stolen databases, not just because it was the largest set, but also because, as a social network, it enabled cybercriminals to target individuals based on their associates and employment. Trial Tr. at 627:5-19. The evidence at trial proved that defendant sold the complete Formspring data set to an individual known as Mehmet Sozen or "Rais" in 2012 and gave LinkedIn email addresses and passwords to accused hacker Oleksandr Ieremenko. The evidence also showed that portions of the LinkedIn, Dropbox, and Formspring databases were all posted publicly at some later point. Defendant thus released users' personal data into the wild, where any cybercriminal could use it to perpetrate new crimes.

The Guidelines offense level does not account for the potential harm to these millions of individuals around the world, and thus, if anything, understates the seriousness of the offenses. The nature and circumstances of his massive data breaches merit a substantial custodial sentence.

B. Defendant's History and Characteristics

Defendant has declined to speak with the Probation Officer who prepared the PSR, but the Court can glean information about him from the proceedings in this case. In particular, the Court will recall that defendant's refusal to work with his retained counsel, and the resulting need for competency proceedings and substitution of panel counsel, caused a significant delay in bringing this case to trial. Defense counsel raised doubts regarding defendant's competency for trial based on his lack of communication with his counsel. Defendant then refused to meet with the psychiatrist retained by his attorneys to assess his competency. Defendant was therefore committed to the custody of the Bureau of Prisons ("BOP") for a competency evaluation. Only when the BOP forensic psychologist, Dr. Lesli Johnson, opined that the defendant was competent to stand trial, did defendant participate in an evaluation by his own expert. The Court held an evidentiary hearing at which both experts testified regarding their opinions. Dr. Johnson found that the defendant's unwillingness to communicate with his attorney was "directly related to his narcissistic traits" and was "volitional and goal-directed." Johnson Report at 20. She reported that he told her at one point "I'm always capable of participating in

conversations, but depending on the situation, the ambience and the people." ECF No. 89 (Transcript of Evidentiary Hearing) at 26:9-14; Johnson Report at 19. When the Court found defendant competent, his retained attorney withdrew, and the Court appointed CJA panel counsel. ECF Nos. 94, 106. Almost a year elapsed from defendant's August 10, 2018, Motion for Psychiatric Exam and Mental Competency Hearing, to the Court's August 6, 2019, appointment of counsel. This delay was the product of defendant's disregard for the Court, the U.S. criminal justice system, and the people working on all sides to ensure his fair trial.

In preparation for sentencing defendant has not expressed remorse or accepted any responsibility for his actions. While declining an interview with the Probation Officer, he has written multiple letters to the Court since his conviction. ECF Nos. 270, 272, 275. In those letters his only concern has been that he be allowed a portable video game system, radio, and MP3 player while in custody. He has also used his letters to confirm some of the evidence introduced against him at trial by the United States, such as his brother's and girlfriend's email addresses, and his own birthday. ECF Nos. 270, 272. The Court should consider this lack of regret on its own, and also consider how it affects the need to deter future crimes by defendant when he returns to Russia.

C. The Need for the Sentence Imposed to Reflect the Seriousness of the Offense, to Promote Respect for the Law, and to Provide Just Punishment for the Offense.

Offenses like defendant's undermine trust in the innovative technology that is the hallmark of the Northern District of California. The Internet has opened up opportunity for billions of people around the world, but also created new and unprecedented opportunities for criminals to steal information on a previously unimaginable scale. Despite that scale, it is important to remember that these crimes affected real people and real companies – for example, Mr. Olonoh testified to the difficulties the breach at Formspring caused to his young company. A computer intrusion and data breach, whether at a large public company or a new venture, can present a serious threat to the viability of the victim business. This type of crime is not merely the moving around of anonymous bytes. The Court's sentence should reflect the seriousness of the threat posed by this type of cybercrime to technology companies and their customers.

//

D. The Need for the Sentence Imposed to Afford Adequate Deterrence and Protect the Public From Further Crimes of the Defendant.

Cybercriminals like defendant operate in online anonymity, insulated behind their keyboards. Cybercriminals in other countries may believe they have an extra layer of protection from U.S. law enforcement. The testimony of United States Secret Service Special Agent Richard LaTulip and FBI Special Agents Anton Mlaker and Jeffrey Miller made clear the challenges of bringing international cybercriminals to justice in the United States. A sentence of 145 months of imprisonment will give pause to criminals around the globe who think they can attack the U.S. economy with impunity. The possibility of conviction and a substantial prison sentence changes the calculus and establishes that the data of U.S. companies is not free for the taking. A Guidelines sentence will provide some measure of general deterrence to the next generation of Yevgeniy Nikulins.

Defendant himself poses an ongoing threat, based on his lack of remorse. When returned to Russia, he will be free to resume his hacking career. A Guidelines sentence of 145 months of imprisonment will protect U.S. companies and global computer users from any further crimes by defendant.

CONCLUSION

For the reasons set forth above, the Court should sentence defendant Nikulin to a Guidelines sentence of 145 months of imprisonment, with restitution to the victim companies as recommended in the PSR. This sentence is sufficient, but not greater than necessary, to achieve the goals of sentencing laid out in 18 U.S.C. § 3553(a).

DATED: September 22, 2020

Respectfully submitted,

DAVID L. ANDERSON
United States Attorney

/s/
MICHELLE J. KANE
KATHERINE L. WAWRZYNIAK
Assistant United States Attorneys